MAC 주소 플랩 알림 오류 트러블슈팅

목차

MAC 주소 플랩 알림

ICSeverity

5 - 알림

영향

전달 루프가 존재하지 않는지 확인하기 위해 이러한 메시지를 조사할 수 있습니다.

설명

이 알림 메시지는 네트워크에서 MAC 주소 플래핑 이벤트를 탐지할 때 스위치에 의해 생성됩니다. 스위치에서 동일한 소스 MAC 주소에서 두 개의 서로 다른 인터페이스로 패킷을 수신할 때 MAC 주소 플래핑 이벤트가 탐지됩니다. Cisco Catalyst 스위치는 여러 스위치 포트에서 동일한 MAC 주소가 탐지될 경우 이를 알림으로써 스위치가 지속적으로 MAC 주소와 연결된 포트를 변경하게 하고, 호스트의 MAC 주소, VLAN 및 MAC 주소가 플래핑되는 포트를 포함하는 이 syslog를 통해 알림을 전송합니다. 이 동작은 여러 가지 이유로 인해 발생할 수 있으므로 네트워크의 안정성과 성능을 보장하려면 MAC 주소 플래핑의 근본 원인을 파악하는 것이 중요합니다.

Syslog 메시지

```
SW_MATM-4-MACFLAP_NOTIF
```

메시지샘플

```
Apr 26 12:27:55 <> %SW_MATM-4-MACFLAP_NOTIF: Host mac address in vlan X is flapping between port PoX an
```

제품군

- Cisco Catalyst 9300 Series 스위치
- Cisco Catalyst 9400 Series 스위치
- Cisco Catalyst 9200 Series 스위치
- Cisco Catalyst 9500 Series 스위치
- Cisco Catalyst 9600 Series 스위치
- Cisco Catalyst 3850 Series Switches
- Cisco Catalyst 3650 Series 스위치
- Cisco Catalyst 6000 Series Switches
- Cisco Catalyst 6800 Series Switches
- Cisco Catalyst 4500 Series Switches
- Cisco Catalyst 4900 Series Switches
- Cisco Catalyst 3750-X Series 스위치
- Cisco Catalyst 3850-X Series 스위치
- Cisco Catalyst 2960 Series Switches

레젝스

해당 없음

권장 사항

이 오류에는 여러 가지 원인이 있을 수 있으며, 그 중 일부는 심각한 네트워크 문제를 나타낼 수 있습니다. 가장 일반적인 세 가지 내용은 아래에 자세히 설명되어 있습니다.

1. 무선 클라이언트 이동(네트워크에 영향을 미치지 않음)

2. 중복 시스템 또는 중복 가상 머신으로부터의 가상 주소 이동(네트워크에 미치는 영향 보통)

3. 레이어 2 루프(네트워크에 미치는 영향이 큼)

#1 세부사항: 무선 클라이언트 이동은 예상된 경우가 많으며, 일반적으로 서비스 영향이 관찰되지 않는 경우 이를 안전하게 무시할 수 있습니다. CAPWAP를 사용하지 않는 AP 간에 로밍하는 클라이언트가 무선 컨트롤러에 다시 연결되거나 서로 다른 두 무선 컨트롤러에 의해 제어되는 AP 간에 로밍하는 경우 이 로그가 생성될 수 있습니다. 동일한 mac 주소에 대해 생성된 로그 간의 시간은 몇 초 또는 몇 분 차이가 날 수 있습니다. 단일 mac 주소가 초당 여러 번 이동하는 경우, 이는 더 심각한 문제를 나타낼 수 있으며 추가 트러블슈팅이 필요할 수 있습니다.

#2 세부사항: 액티브/스탠바이 상태로 작동하는 일부 이중화 시스템 또는 디바이스는 특정 시점에 액티브 디바이스만 사용하여 공통 가상 IP 및 mac 주소를 공유할 수 있습니다. 두 디바이스가 예기치 않게 활성화되고 두 디바이스 모두 가상 주소 사용을 시작하는 경우 이 오류가 표시될 수 있습니다. 로그에 언급된 인터페이스 조합과 show mac address-table address vlan 명령을 사용하면 네트

워크를 통해 이 mac의 경로를 추적하여 어디에서 어떤 디바이스가 공유 mac에서 트래픽을 생성하는지 확인할 수 있습니다. 이동을 생성하는 디바이스의 특성에 따라 이중화 상태의 추가 트러블슈팅이 필요할 수 있습니다. #3 세부사항: L2 루프는 종종 매우 짧은 시간 동안 많은 수의 mac 이동 오류를 생성합니다(초당 하나 이상, 더 많은 경우). 로그는 일반적으로 단일 또는 소수의 mac 주소에 사용될 수 있으며, 사용자는 네트워크에 영향을 미칠 수 있습니다. 라우팅 및 레이어 2 프로토콜이 실패할 경우 추가 로그가 생성되고 일반 불안정성이 발생할 수 있습니다. L2 루프 문제를 해결하려면 show int 명령을 실행합니다 | in은 up|입력 속도이며 초당 매우 많은 양의 입력 패킷을 표시하는 모든 활성 인터페이스를 기록합니다(일반적으로 인터페이스의 속도에 따라 6, 7 또는 8 이상의 매우 큰 숫자 수). 입력 속도가 비정상적으로 높은 인터페이스는 1개 또는 2개에 불과할 수 있습니다. 출력 속도에 초점을 맞추지 말고 스패닝 트리 TCN에 초점을 맞추지 마십시오. 하이 입력 인터페이스가 식별되면 CDP, LLDP 또는 인터페이스 설명/네트워크 다이어그램을 사용하여 해당 포트에 연결된 인접 디바이스에 로그인하고 show int를 실행합니다 | in is up|input rate 명령을 다시 수행하고 비정상적인 입력 속도로 인터페이스를 추적하는 프로세스를 반복합니다. 네트워크를 통해 추적할 때 인터페이스와 호스트 이름을 추적합니다. 입력 포트가 부족해질 때까지 인접 디바이스를 계속 점검하고 입력 속도를 확인합니다. 그러면 인접 디바이스가 부족해지거나 이미 확인한 디바이스로 돌아갑니다. 이 방법론 중에 두 가지 가능한 결과 중 하나가 발생할 수 있습니다. CDP, LLDP 또는 알려진 인접 디바이스가 없지만 매우 높은 입력 속도가 있는 포트로 끝날 경우 관리상 해당 포트를 종료합니다. 이 인터페이스는 궁극적인 소스이거나 루프에 대한 기여자일 가능성이 높습니다. 네트워크가 안정화될 때까지 60초 동안 기다린 후 루프 상태가 계속 표시되면 인터페이스를 종료하고 프로세스를 다시 시작합니다. 네트워크에 두 번째 소스가 있는 것이 원인일 수 있습니다. 이미 선택한 디바이스에서 종료한 경우, 이는 사용 중인 루프 방지 프로토콜(스패닝 트리가 가장 일반적임)이 어딘가에서 실패했음을 나타냅니다. 스패닝 트리 네트워크의 경우, 추적한 경로의 어떤 스위치가 루트여야 하는지 확인하고 해당 디바이스에서 역방향으로 작업하여 추적된 경로 내에서 어떤 인터페이스가 차단 상태에 있을 수 있는지 확인합니다. 차단할 수 있지만 포워딩 상태에 있는 인터페이스가 발견되면 관리상 해당 인터페이스를 종료합니다. 60초 동안 기다렸다가 네트워크의 안정성을 확인합니다. 루프가 지속되면 인터페이스를 종료하고 이 프로세스를 반복합니다.

명령

#show version

#show logging

#show spanning-tree

#show mac-address-table

#show mac address-table

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.